Malware

Hello

Toomas Lepik

Information Security Expert

Communication for course

course-malware@cert.ee

Expectations

Interactive

attendance

I will make mistakes and encourage you finding them :)

Labs are extension for course where you can all-sow play with computers

Things I hope we learn

Malware

- Malware classification
- Modern attack trends (attacker strategies)
- General concepts for organization protection
- Commonality available resources
- Malware Incident handling
- Black boxing introduction

Malware2

- All things that we could not cover as deep as I'd liked
- Black boxing
- Reverse engineering
- Memory analysis

what it is Malware ?

Malware

Malware, short for malicious software, is software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code

http://en.wikipedia.org/wiki/Malware

Malware

Software is considered to be malware based on the perceived intent of the creator rather than any particular features

http://en.wikipedia.org/wiki/Malware


STAR ALLIANCE
Spanair

http://www.space.com/news/080827-iss-computervirus.html

http://www.theregister.co.uk/2010/08/20/spanair_malware/

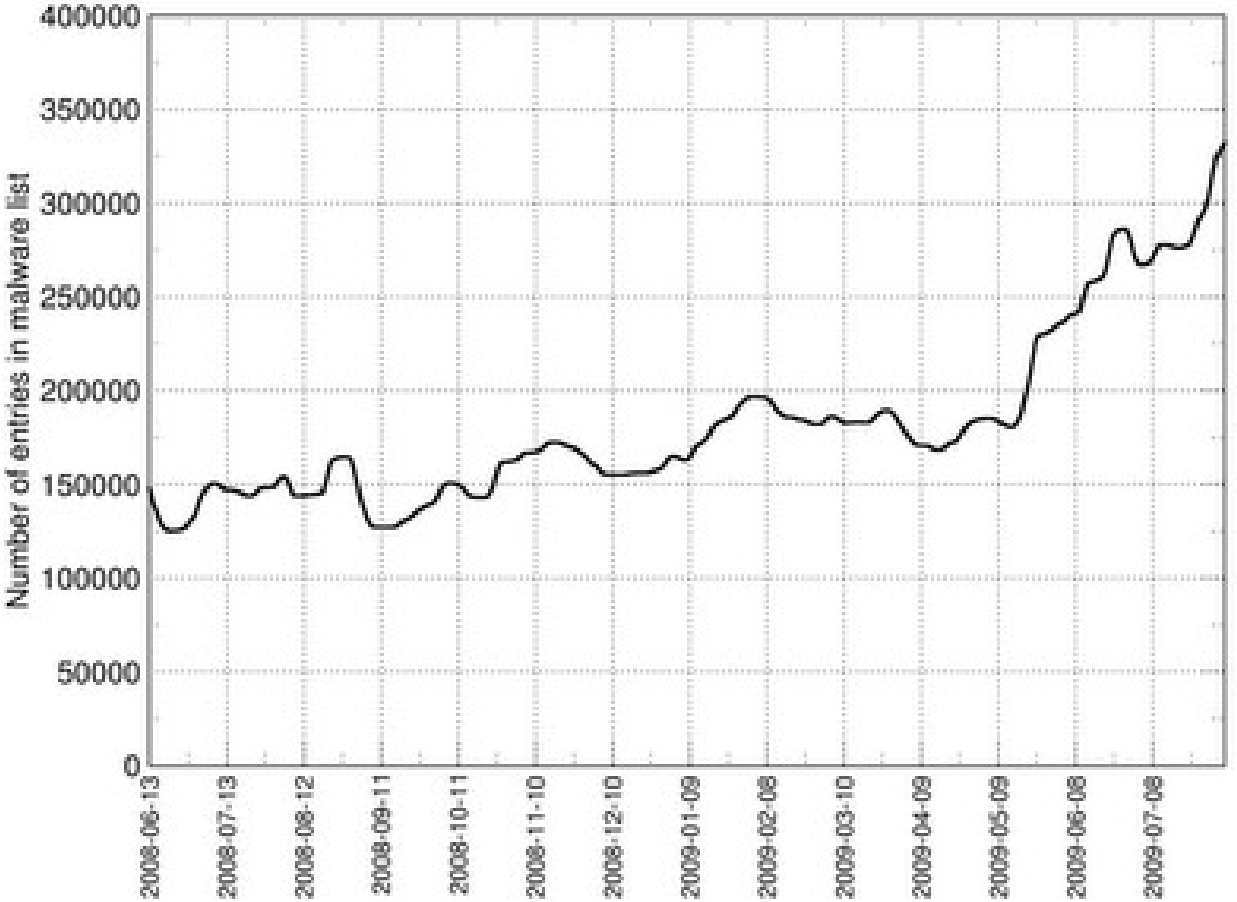
http://www.theregister.co.uk/2009/01/15/royal_navy_email_virus_outage/

Measuring the in-the-wild effectiveness of Antivirus against Zeus

Trusteer

September 14, 2009

In other words, installing an anti-virus product and maintaining it up to
date reduces the probability to get infected by Zeus by 23%, compared
to running without an anti-virus altogether

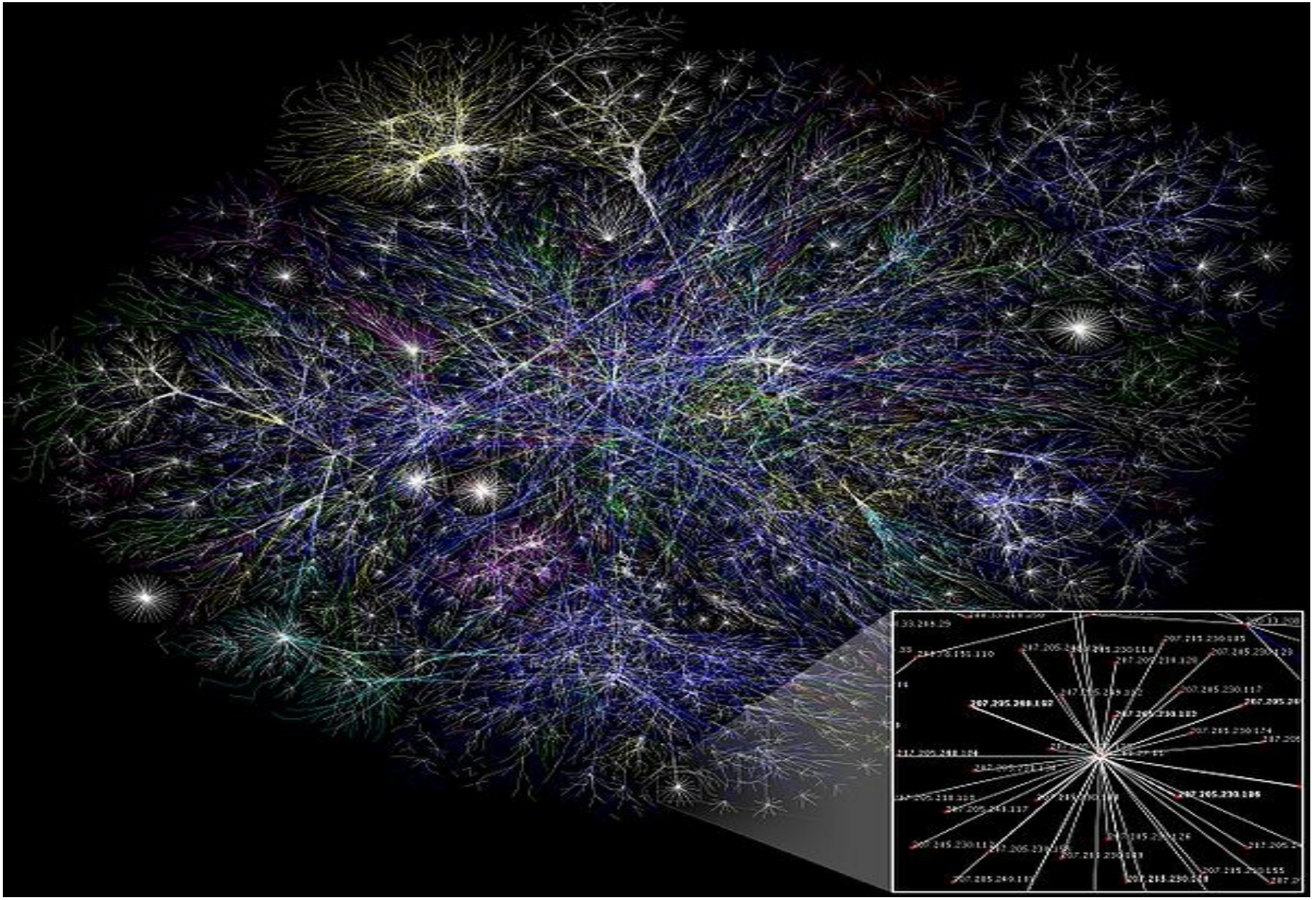


http://googleonlinesecurity.blogspot.com/2009/08/malware-statistics-update.html


ПИЗДЕЦ
БЕЗ ВАРИАНТОВ


WHAT CAN I DO TO AVOID GETTING COMPUTER VIRUSES?
GIVE YOUR POWER CORD A SPINAL ADJUSTMENT ONCE A WEEK TO PREVENT DISEASE.
I WAS SKEPTICAL UNTIL HE SAID THERE'S ANECDOTAL EVIDENCE THAT IT WORKS!
www.dilbert.com scottadams@aol.com
1/06/02 © 2002 United Feature Syndicate, Inc.

Enviroment



IP address

- IP = Internet Point
- xxx.yyy.zzz.qqq , 4 baits, 0..255
- ***nslookup sigalind.homeip.net*** – 82.131.29.201
- 394.902.304.1 ?
- … IPv4

IP v6

- **2001:0db8:ac10:fe01:0000:0000:0000:0000**
- Notation: 16 bait
- transport mode, tunnel mode
- Built in cryptoi capability : HMA1 SHA1 / Triple DES CBC, AES CBC
- … juba 10 aastat tulekul

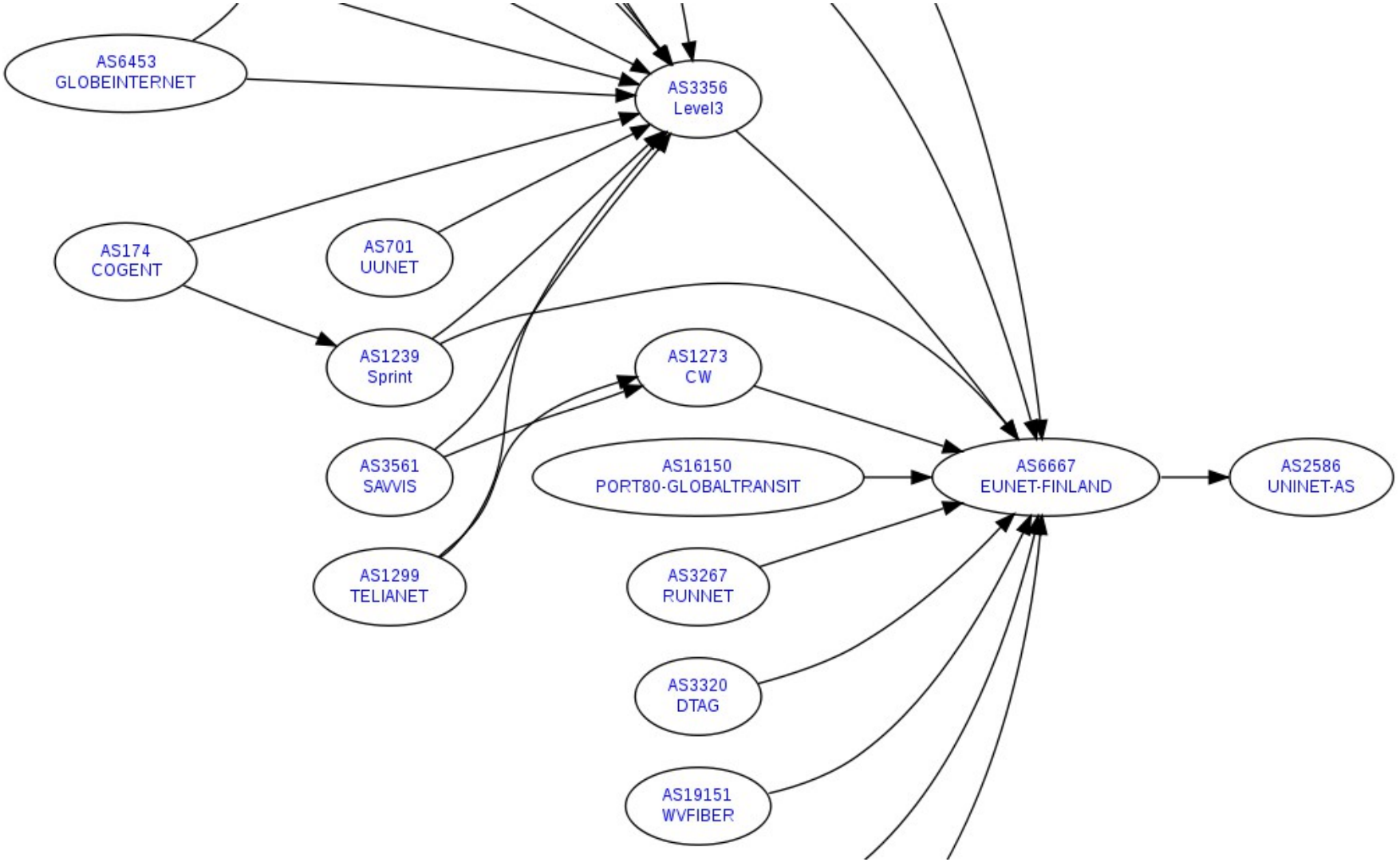
Resources and responsibility

- **ICANN** - The Internet Corporation for Assigned Names and Numbers
- **RIPE NCC** - Réseaux IP Européens Network Coordination Centre - allocation and registration of Internet number resources (IP Addresses and AS Numbers)
- EIS? → abcdefg.ee
- TJA? → +(372) 6655771; 100,7MHz
- EÜ? Government? Polis? Court?

Procedure

- www.ripe.net
- ISP TransDnistriasse (ZEUS / BlackHat)
- OÜ Mees ja Koer (does not have to be ISP)
- Extra small size: 1300EUR user fee + 2000EUR administration fee
- LIR = Local Internet Registrar

AS (Autonomous System)



Merchandise

- An ASN, or Autonomous System Number, is usually technically defined as a number assigned to a group of network addresses, managed by a particular network operator, sharing a common routing policy.
  - In real-time BGP exchange
    - Between AS111 and AS222.l
- Thins that we can get:
  - One AS number (ASN) AS5555555
  - One IP range 555.555.555.0/22
  - We a registred in RIPE ?

whois AS3327

```
admin-c:          LNO5-RIPE
tech-c:           LNO5-RIPE
mnt-routes:       AS3327-MNT
mnt-by:           AS3327-MNT
source:           RIPE # Filtered

role:             Linxtelecom Network Operations
address:          Linxtelecom Estonia
address:          Mustamae tee 46
address:          10621 Tallinn
address:          ESTONIA
phone:            +372 622 3370
phone:            +372 517 8778
fax-no:           +372 654 2942
abuse-mailbox:    abuse@linxtelecom.ee
admin-c:          MV88-RIPE
tech-c:           AL2221-RIPE
tech-c:           RA1683-RIPE
tech-c:           SAM22-RIPE
tech-c:           PA5112-RIPE
nic-hdl:          LNO5-RIPE
mnt-by:           AS3327-MNT
source:           RIPE # Filtered
```